The History of Lagrange's Theorem for Finite Groups

Matthew Bourke Shane Doyle Dylan Gallagher

Introduction

This poster conveys the journey through time, and the evolution of Lagrange's theorem from beginning as an observation on the permutations of the values of an equation to its modern applications to abstract group.

Timeline

1761 Euler publishes proof for Fermat's Little Theorem

1770 Lagrange attempts to find a formula to solve a general quintic equation in his *"Re- flexions sur la resolution algebrique des equation"*

1799 Ruffini claims no quintic equation exists

1801 Gauss proves Lagrange's Theorem to be true for the special case of $\frac{\mathbb{Z}}{p\mathbb{Z}}$

1815 Cauchy launches Permutation Group Theory as an independent topic

1820 Abel formally proves Ruffini's statement

1831 Galois introduces the term "Group" for the study of these topics

1844 Cauchy proves Lagranges Theorem for the symmetric group S_n

1861 Jordan proves Lagrange's Theorem more generally for any abstract group

1949 English Version of Van der Waerden's *"Moderne Algebra"* attributes the Theorem to Lagrange

Lagranges Theorem

For a finite group G the order of any subgroup H divides the order of G, i.e. the number of elements in H is a factor of the number of elements in G.

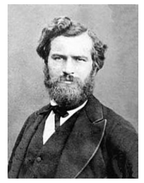
Original Thinking

- Lagrange originally attempted to find a general formula to solve a general quintic equation
- He discovered that an equation of the form $x_1x_2 + x_3x_4$ could only be permuted into 3 possible values (a divisor of 4! = 24 the number of permutations of 4 elements).

Cauchy and Galois

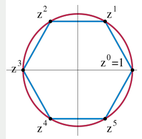
- Cauchy wrote a paper on permutation groups, before the idea of a group was formalised.
- Galois introduced the term 'group' in a paper on solving solutions of polynomials by radicals in 1831, formalising the idea of a group.

Jordan



Jordan proved that Lagranges Theorem applies in the case of any permutation group in 1861

Examples of Lagranges Theorem



Lagranges Theorem can be seen in action for the group of 6^{th} roots of unity which has all proper subgroups of order 2 or 3 a factor of 6.

Lagrange's Personal History

RÉFLEXIONS

SUR LA

RÉSOLUTION ALGÉBRIQUE DES ÉQUATIONS[*].

- Born in Turin on the 25^{th} of January 1736.
- Lagrange's interest in mathematics originated from a chance reading of a memoir by English astronomer Edmond Halley when he was just 17.
- Solved the isoperimetrical problem at the age of 19 in a letter to Euler.
- Lagrange famously said that "If I had been rich, I probably would not have devoted myself to mathematics".
- In 1766 Euler left Berlin, and Frederick the Great immediately wrote expressing his wish to have "the greatest mathematician in Europe" resident at his court.
- Lagrange died in Paris on the 10^{th} of April 1813.

Fermat's Little Theorem

If p is prime b relatively prime to p then $b^{p-1} \equiv 1$
This is an example of Lagranges Theorem for $\frac{\mathbb{Z}}{p\mathbb{Z}}$ (the multiplicative group of the integers relatively prime to p, modulo p)
This has many modern day uses in the field of cryptography, being used for cyber-security cryptocurrencies such as Bitcoin

NUI Galway
OÉ Gaillimh

References

Roth, Richard L. "A History of Lagrange's Theorem on Groups." Mathematics Magazine, vol. 74, no. 2, 2001, pp. 99–108. JSTOR, www.jstor.org/stable/2690624.
W. W. Rouse Ball, 1908, "Joseph Louis Lagrange (1736–1813)" A Short Account of the History of Mathematics, 4th ed. Gutenberg http://www.gutenberg.org/ebooks/31246